UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* One cellular phone, as more fully described in Attachment A	)	Case No. MJ23-522

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

One cellular phone, as more fully described in Attachment A, attached hereto and incorporated herein by reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, attached hereto and incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 2115	Attempted Burglary of the United States Post Office

The application is based on these facts:

✓ See Affidavit of Inspector Kelsie P. Shaphren, USPIS, continued on the attached sheet.

☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☑ by reliable electronic means; or: ☐ telephonically recorded.

Applicant's signature

Inspector Kelsie P. Shaphren, USPIS

Printed name and title

◯ The foregoing affidavit was sworn to before me and signed in my presence, or

◉ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 10/26/2023

Judge's signature

City and state: Seattle, Washington

Brian A. Tsuchida, United States Magistrate Judge

Printed name and title

ATTACHMENT A

The property to be searched is a cellular telephone with Motorola telephone SIM card TF256PSIMV97N 89148000008152850123, hereinafter the "SUBJECT DEVICE." The SUBJECT DEVICE is currently located at USPIS Seattle Domicile, 301 Union Street, Seattle, WA 98101.

This warrant authorizes the forensic examination of the SUBJECT DEVICE for the purpose of identifying the electronically stored information described in Attachment B.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

1. All records on the SUBJECT DEVICE described in Attachment A that relate to violations of Title 18, United States Code, Section 2115, Attempted Burglary of a Post Office, those violations occurring on or about October 10, 2023, including:

a. The assigned number to the SUBJECT DEVICE (known as mobile directory number or MDN) and the identifying telephone serial number (such as Mobile Identification Number or MIN; Electronic Serial Number or ESN; International Mobile Subscriber Identity or IMSI; and/or International Mobile Equipment Identity or IMEI);

b. Service provider information of the SUBJECT DEVICE;

c. Subscriber information of the owner of the SUBJECT DEVICE, including but not limited to phone number, name, address, and dates of service;

d. Stored list of recent received, sent, or missed calls;

e. Stored contact information;

f. Photographs and videos related to the above crime;

g. Photographs and videos that may show the owner of the SUBJECT DEVICE and/or co-conspirators, including any embedded GPS data associated with these photographs;

h. Stored text messages related to the above crime including Apple iMessages, Blackberry Messenger messages or other similar messaging services where the data is stored on the telephone; and

i. Location data stored on the SUBJECT DEVICE, including data from GPS navigation applications.

2. Evidence of user attribution showing who used or owned the SUBJECT DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of digital device or electronic storage (such as flash memory or other media that can store data) and any photographic form.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

AFFIDAVIT OF KELSIE P. SHAPHREN

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, Kelsie P. Shaphren**,** having been duly sworn, state as follows:

INTRODUCTION AND INSPECTOR BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of a digital device[1] or other electronic storage media,[2] hereinafter the "SUBJECT DEVICE," which is currently in law enforcement possession, and the extraction from that device or electronic storage media of electronically stored information described in Attachment B.

2. I am a Postal Inspector with the United States Postal Inspection Service (USPIS) and have been since November 18, 2022. During my Basic Inspector Training, I learned how to investigate and support the prosecution of postal-related crimes, including mail theft, identify theft, mail fraud, narcotics offenses, and violent crimes such as assault, robberies, burglaries, and homicides. In November 2022, I was assigned to the

[1] "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

[2] Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Seattle Division's Mail Theft and Mail Fraud Team. I investigate any offenses involving the U.S. Mail, USPS employees, and our customers in Seattle.

3. Since joining the Seattle Division's Mail Theft and Mail Fraud Team, I completed an Advanced Robbery and Burglary training, which includes familiarization with cellular telephone search warrants and other technical device warrants.

4. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience.

5. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits and instrumentalities of violations of Title 18, United States Code 2115, Attempted Burglary of a Post Office will be found on the SUBJECT DEVICE.

IDENTIFICATION OF THE SUBJECT DEVICE TO BE EXAMINED

6. The SUBJECT DEVICE is a cellular telephone with Motorola telephone SIM card TF256PSIMV97N 89148000008152850123. The SUBJECT DEVICE is currently located at USPIS Seattle Domicile, 301 Union Street, Seattle, WA 98101.

7. The warrant would authorize the forensic examination of the SUBJECT DEVICE for the purpose of identifying electronically stored data particularly described in Attachment B.

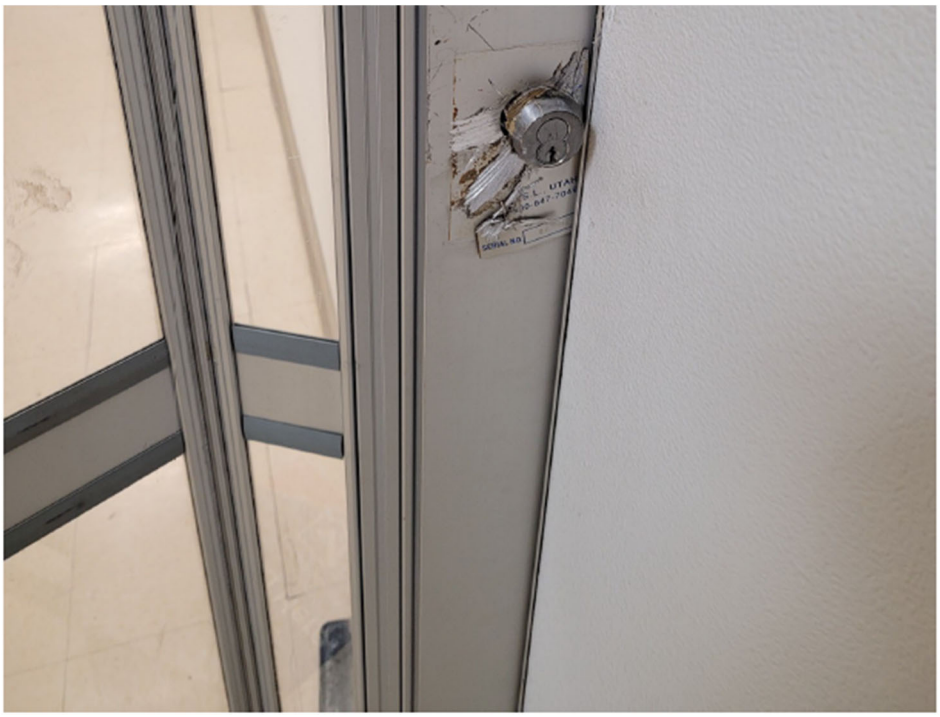
UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

THE INVESTIGATION

8. On or about October 10, 2023, there was an attempted burglary of the Brinnon Post Office, located at 144 Brinnon Lane, Brinnon, WA 98320. At approximately 8:30 AM, Postmaster S.H. contacted USPIS to report the incident.

9. Deputy Jason Avery of the Jefferson County Sheriff's Office (JCSO) was the responding officer. I arrived at the Brinnon Post Office at approximately 11:00 AM.

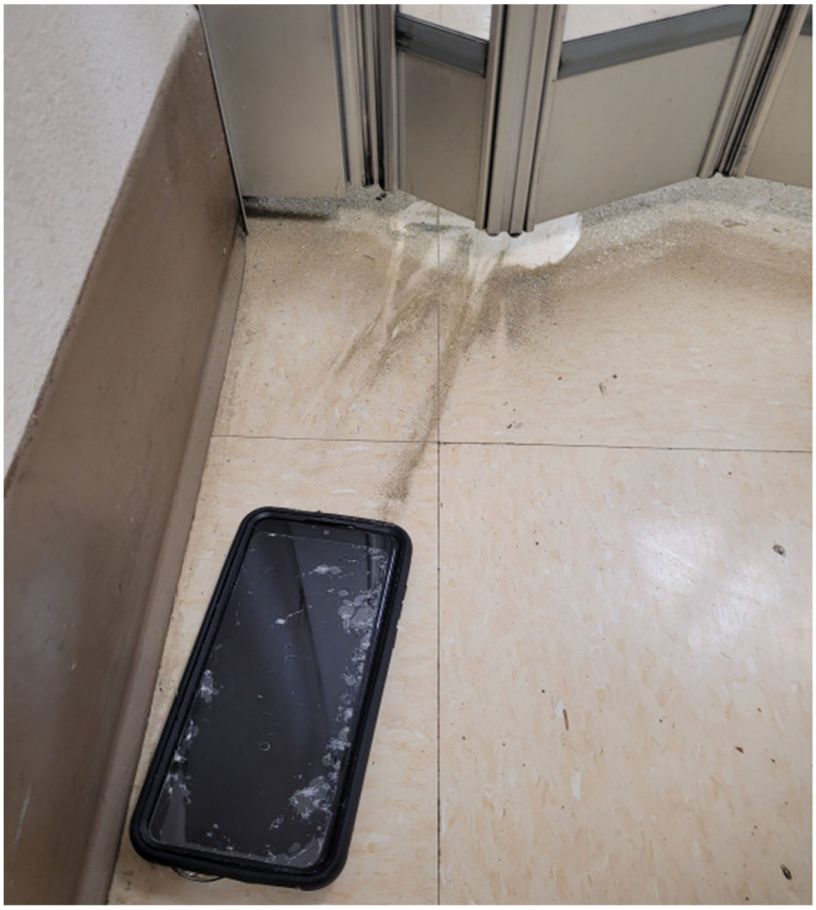
10. According to Deputy Jason Avery, he saw that the security partition had visible damage on the lower track pins and the tumbler lock, and that there were dust and debris covering the floor around the security partition. At the Brinnon Post Office, the security partition divides the 24-hour access lobby containing post office boxes from the counter service area with unrestricted access to with mail, cash registers, and a safe. Deputy Avery believed someone used a power tool, such as a grinding tool, to attempt to cut through the security partition's locking mechanisms but failed to do so.



The tumbler lock with visible damage

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

11. Deputy Avery located the SUBJECT DEVICE on the opposite side of the security partition—the secured side of the partition that was not accessible by the public. There were visible slide marks in the dust and debris under the damaged tumbler lock, which suggested the SUBJECT DEVICE slid under the security partition after the tumbler lock had been damaged and became out of reach of the SUBJECT DEVICE's owner. Deputy Avery retained the SUBJECT DEVICE as evidence.



Taken from the secured side of the security partition. This photo shows the SUBJECT DEVICE and slide marks in the dust and debris.

12. There are no security cameras in the Brinnon Post Office or the surrounding parking lot. As of October 18, 2023, the Brinnon Post Office has not received any inquiries about the SUBJECT DEVICE, and no one has come forward to claim the SUBJECT DEVICE.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

13. Based on my training and experience, I believe that the SUBJECT DEVICE was likely dropped by the person who attempted to break into the secured side of the security partition and to burglarize the Brinnon Post Office.

14. Accessing the SUBJECT DEVICE will help law enforcement determine the owner of the SUBJECT DEVICE and investigate the attempted burglary of the Brinnon Post Office. The SUBJECT DEVICE may also contain evidence relevant to the planning of the attempted burglary of the Brinnon Post Office, as explained below.

15. Based on my training, experience, and conversations with other law enforcement officers involved in burglary investigations, I know that individuals planning burglaries use cellular telephones as a tool or instrumentality in committing their criminal activity. They use cellular telephones to maintain contact with co-conspirators, to research potential businesses to burglarize, to obtain the address of those businesses, to generate directions to those businesses, and to take photographs of the businesses prior to attempting burglaries and of stolen items taken during the burglaries. As a result, evidence of a burglary or attempted burglary can often be found in text messages, call logs, photographs, videos, and other stored data on the cellular phone.

16. The SUBJECT DEVICE is currently in the lawful possession of the USPIS. It came into the USPIS's possession after Jefferson County Sheriff's Office retained the SUBJECT DEVICE as evidence of a potential crime and transferred it to USPIS.

17. The SUBJECT DEVICE is currently in storage at USPIS Seattle Domicile, 301 Union Street, Seattle, WA 98101. Based on my training and experience, I know that the SUBJECT DEVICE has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the SUBJECT DEVICE first came into the possession of the USPIS.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

TECHNICAL TERMS

18. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a digital device connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

19. Based on my training, experience, and research, I know that the SUBJECT DEVICE has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

DIGITAL DEVICE, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

20. Based on my knowledge, training, and experience, I know that digital devices and electronic storage media can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device used to access the Internet. This information can sometimes be recovered with forensic tools.

21. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the SUBJECT DEVICE was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the SUBJECT DEVICE because:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. As explained herein, information stored within a digital device and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a digital device or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the digital device or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the digital device was remotely accessed, thus inculpating or exculpating the device owner and/or others with direct physical access to the device. Further, digital device and storage media activity can indicate how and when the digital device or storage media was accessed or used. For example, as described herein, digital devices typically contain information that log: digital device user account session times and durations, device activity associated with user accounts, electronic storage media that connected with the device, and the IP addresses through which the device accessed networks and the internet. Such information allows investigators to understand the chronological context of digital device or electronic storage media access, use, and events relating to the crime under investigation.[3] Additionally, some

[3] For example, if the examination of a digital device shows that: a) at 11:00am, someone using the device used an internet browser to log into a bank account in the name of John Doe; b) at 11:02am the internet browser was used to download child pornography; and c) at 11:05 am the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

information stored within a digital device or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a wireless telephone may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the digital device user. Last, information stored within a digital device may provide relevant insight into the device user's state of mind as it relates to the offense under investigation. For example, information within the digital device may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the digital device or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a digital device is evidence may depend on other information stored on the device and the application of

---

internet browser was used to log into a social media account in the name of John Doe, an investigator may reasonably draw an inference that John Doe downloaded child pornography.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

22. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

DIGITAL DEVICES AS INSTRUMENTALITIES OF THE CRIMES

23. Based on my training and experience, the data maintained in the SUBJECT DEVICE may include evidence of a crime or crimes. This includes the following:

a. The assigned number to the SUBJECT DEVICE (known as the mobile directory number or MDN) and the identifying telephone serial number (such as Mobile Identification Number or MIN; Electronic Serial Number or ESN; International Mobile Subscriber Identity or IMSI; and/or International Mobile Equipment Identity or IMEI) are important evidence because they reveal the service provider, allow me to obtain subscriber information, and uniquely identify the telephone. This information can be used to obtain call records and to identify other telephones used by the same subscriber or purchased as part of a package.

b. The stored list of recent received, sent, or missed calls and stored contact information are important evidence. They identify telephones recently in contact with the owner of the SUBJECT DEVICE and can lead to friends and associates who can identify, help locate, and provide information about the owner of the SUBJECT DEVICE.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

c. Stored text messages are important evidence. Based on my experience and training, individuals who commit burglaries or attempted burglaries often communicate with their co-conspirators via text messages to discuss their plans.

d. Photographs and videos stored on the SUBJECT DEVICE are important evidence because they help identify the owner of the SUBJECT DEVICE, either through his or her own picture, or through pictures of friends, family, and associates who can identify the user. It is also likely that photographs of stolen postal property are stored on the SUBJECT DEVICE. Based on my training and experience, I know that individuals who commit post office burglaries take photographs or videos of post offices and stolen items, mail, and keys for future use. In addition, digital photographs and videos have GPS data (i.e., the longitude and latitude of the location at which a photograph or video is taken) embedded in them, and this information can have evidentiary value because it shows the whereabouts of the owner of the SUBJECT DEVICE leading up to and during the attempted burglary of the Brinnon Post Office.

e. Information found in any GPS navigation applications stored on the SUBJECT DEVICE is also important because it will show the whereabouts of the owner of the SUBJECT DEVICE leading up to and during the attempted burglary of the Brinnon Post Office.

SEARCH TECHNIQUES

24. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for will permit imaging or otherwise copying all data contained on the SUBJECT DEVICE and will specifically authorize a review of the media or information consistent with the warrant.

25. In accordance with the information in this affidavit, law enforcement personnel will execute the search of the SUBJECT DEVICE pursuant to this warrant as follows:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

a. Securing the Data

i. In order to examine the ESI in a forensically sound manner, law enforcement personnel with appropriate expertise will attempt to produce a complete forensic image, if possible and appropriate, of the SUBJECT DEVICE.[4]

ii. Law enforcement will only create an image of data physically present on or within the SUBJECT DEVICE. Creating an image of the SUBJECT DEVICE will not result in access to any data physically located elsewhere. However, SUBJECT DEVICE that have previously connected to devices at other locations may contain data from those other locations.

b. Searching the Forensic Images

i. Searching the forensic images for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement may need to conduct more extensive searches to locate evidence that falls within the scope of the warrant. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this affidavit.

---

[4] The purpose of using specially trained computer forensic examiners to conduct the imaging of digital devices or other electronic storage media is to ensure the integrity of the evidence and to follow proper, forensically sound, scientific procedures. When the investigative agent is a trained computer forensic examiner, it is not always necessary to separate these duties. Computer forensic examiners often work closely with investigative personnel to assist investigators in their search for digital evidence. Computer forensic examiners are needed because they generally have technological expertise that investigative agents do not possess. Computer forensic examiners, however, often lack the factual and investigative expertise that an investigative agent may possess on any given case. Therefore, it is often important that computer forensic examiners and investigative personnel work closely together.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ii. These methodologies, techniques, and protocols may include the use of a "has value" library to exclude normal operating system files that do not need to be further searched.

CONCLUSION

26. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the SUBJECT DEVICE described in Attachment A to seek the items described in Attachment B.

27. The affidavit and application are being presented by reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41(d)(3).

Kelsie P. Shaphren
Postal Inspector
United States Postal Inspection Service

The above-named inspector provided a sworn statement to the truth of the foregoing affidavit by telephone on 26 day of October, 2023.

The Honorable Brian A. Tsuchida
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A

The property to be searched is a cellular telephone with Motorola telephone SIM card TF256PSIMV97N 89148000008152850123, hereinafter the "SUBJECT DEVICE." The SUBJECT DEVICE is currently located at USPIS Seattle Domicile, 301 Union Street, Seattle, WA 98101.

This warrant authorizes the forensic examination of the SUBJECT DEVICE for the purpose of identifying the electronically stored information described in Attachment B.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

1. All records on the SUBJECT DEVICE described in Attachment A that relate to violations of Title 18, United States Code, Section 2115, Attempted Burglary of a Post Office, those violations occurring on or about October 10, 2023, including:

a. The assigned number to the SUBJECT DEVICE (known as mobile directory number or MDN) and the identifying telephone serial number (such as Mobile Identification Number or MIN; Electronic Serial Number or ESN; International Mobile Subscriber Identity or IMSI; and/or International Mobile Equipment Identity or IMEI);

b. Service provider information of the SUBJECT DEVICE;

c. Subscriber information of the owner of the SUBJECT DEVICE, including but not limited to phone number, name, address, and dates of service;

d. Stored list of recent received, sent, or missed calls;

e. Stored contact information;

f. Photographs and videos related to the above crime;

g. Photographs and videos that may show the owner of the SUBJECT DEVICE and/or co-conspirators, including any embedded GPS data associated with these photographs;

h. Stored text messages related to the above crime including Apple iMessages, Blackberry Messenger messages or other similar messaging services where the data is stored on the telephone; and

i. Location data stored on the SUBJECT DEVICE, including data from GPS navigation applications.

2. Evidence of user attribution showing who used or owned the SUBJECT DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of digital device or electronic storage (such as flash memory or other media that can store data) and any photographic form.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970